(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
H04L 9/00

(11) 공개번호 특2001-0004137
(43) 공개일자 2001년01월15일

(21) 출원번호 10-1999-0024751
(22) 출원일자 1999년06월28일

(71) 출원인 삼성전자 주식회사 윤종용
경기도 수원시 팔달구 매탄3동 416
(72) 발명자 김도형
경기도화성군봉담면수기리1-93
(74) 대리인 이영필, 권석흥, 이상용

심사청구 : 없음

(54) 불법 복제 방지를 위한 디지털 인터페이스 방법

요약

본 발명은 디지털 인터페이스 방법에 관한 것으로서, 특히 디지털 인터페이스를 통해 소오스(source)와 싱크(sink) 기기가 연결되어 있는 경우에 저작권 보호를 위한 정상적인 프로토콜의 과정을 거치지 않고 불법 복제를 시도하는 경우에 불법 복제 방지를 위한 디지털 인터페이스 방법에 관한 것이다.

본 발명에 의하면 불법 복제로부터 보호할 필요성이 있는 콘텐츠가 디지털 인터페이스를 통해 소오스 기기와 싱크 기기 사이에서 전송되는 경우에 싱크 기기가 불법 복제 방지 프로토콜에 따라 일정 시간이내에 상호인증요구를 송신하지 않으면 콘텐츠의 전송 중단, 소오스 기기에서 싱크 기기로의 상호인증요구, 또는 암호 변경 등을 실행함으로써, 불법 복제 시도를 무력화시킬 수 있는 효과가 있다.

대표도

도4

명세서

도면의 간단한 설명

도 1은 IEEE 1394의 프로토콜 스택(protocol stack)을 도시한 것이다.

도 2는 종래의 기술에 의한 불법 복제를 방지하기 위한 디지털 트랜스미션 콘텐츠 프로텍션 프로토콜의 기본 구조를 도시한 것이다.

도 3은 본 발명이 적용된 일 실시 예에 의한 IEEE 1394 네트웍의 구성도이다.

도 4는 본 발명의 제1실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법을 설명하기 위한 프로토콜의 구조를 도시한 것이다.

도 5는 본 발명의 제2실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법을 설명하기 위한 프로토콜의 구조를 도시한 것이다.

도 6은 본 발명의 제3실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법을 설명하기 위한 프로토콜의 구조를 도시한 것이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 디지털 인터페이스 방법에 관한 것으로서, 특히 디지털 인터페이스를 통해 소오스(source)와 싱크(sink) 기기가 연결되어 있는 경우에 저작권 보호를 위한 정상적인 프로토콜의 과정을 거치지 않고 불법 복제를 시도하는 경우에 불법 복제 방지를 위한 디지털 인터페이스 방법에 관한 것이다.

최근들어 디지털 TV, 디지털 VCR, 디지털 셋톱박스(SETUP BOX) 등 각종 디지털 기기들이 등장하고 있으며, 이들 디지털 기기들이 서로 인터페이스하여 통신할 수 있는 네트웍인 IEEE 1394가 각광을 받고 있는 추세이다.

도 1은 IEEE 1394의 프로토콜 스택(protocol stack)을 도시한 것으로서, 1394 통신 기능을 채용한 각 기

기들이 갖추고 있는 일반적인 프로토콜 스택은, 최하위층인 물리 계층(phisycal layer :100), 링크 계층(link layer :110), 트랜잭션 계층(transaction layer :120) 및 최상위층인 시리얼 버스 매니지먼트(Serial Bus Management :130)로 이루어진다. 물리 계층(100)은 송신시 링크 계층(110)으로부터 비트열을 전달받고, 시리얼 버스의 사용권을 획득한 뒤 이를 인코딩하고 전기적 신호로 변환하여 외부 버스상으로 데이터를 전송한다. 수신시에는 이와 반대의 과정을 거친다. 링크 계층(110)은 패킷단위로 데이터를 다루며, 패킷의 구성 및 분해, 에러 검출, 버스 사이클 관리 기능을 가진다. 일반적으로 물리계층(100)과 링크 계층(110)은 칩셋(chipset)으로 구성된다. 트랜잭션 계층(120)은 데이터 읽기/쓰기/잠금(lock)과 같은 트랜잭션을 제공하며 하위층에서 제공되는 서비스를 이용하여 1394 버스상에 놓인 다른 디바이스(또는 노드)와 비동기 통신을 수행한다. 시리얼 버스 매니지먼트(130)는 컨피규레이션(configuration) 롬(ROM)이나 CSR(Control and Status Register) 등과 같은 여러가지 자료구조를 내장하며, 파워 관리, 버스상에 연결되는 시스템 전체의 연결구조/스피드 맵 등과 같은 최상위층의 관리 역할을 담당한다. 트랜잭션 계층(120) 및 시리얼 버스 매니지먼트 계층(130)은 소프트웨어로 작성되어지며, 각 디바이스의 마이크로프로세서에 내장되어 구현된다.

이와 같은 IEEE 1394 디지털 인터페이스를 통해 소오스 기기와 싱크 기기가 연결되어 있는 경우에 이들 간에 전달되는 콘텐츠(contents)가 저작권 보호를 요구하는 것인 경우에는 소오스 기기와 싱크 기기 사이에 상호인증과정을 거쳐서 안전한 암호채널을 형성하고 이 암호채널을 통해서 콘텐츠가 전달되게 된다.

도 2는 종래의 기술에 의한 불법 복제를 방지하기 위해 전세계적으로 논의되고 있는 디지털 트랜스미션 콘텐츠 프로텍션 프로토콜(digital transmission contents protection protocol)의 기본 구조이다.

즉, 초기에 싱크 기기로부터 소오스 기기에 콘텐츠 전송 요구가 전달되면, 소오스 기기는 전송해야 할 저작권 정보를 보고 이 정보가 "copy-free"가 아니라 저작권 보호를 요구하는 내용인 경우에는 이 콘텐츠의 스트림을 암호화 모듈을 사용하여 암호화하고 여기에 저작권 정보(Encryption Mode Indicator :EMI)를 덧붙인 후 IEEE 1394와 같은 디지털 인터페이스를 통해서 싱크 기기로 전송한다(단계①). 그러면, 싱크 기기는 수신되는 콘텐츠 스트림의 저작권 정보를 보고 이 정보가 "copy-free"가 아닌 경우에는 이 콘텐츠 스트림이 암호화되어 있는 것으로서 현재로는 무용(useless)한 것으로 판단하고 소오스 기기로 상호인증(authentication)을 요구한다(단계②). 싱크 기기로부터 소오스 기기로 상호인증요구가 전해지면, 싱크 기기와 소오스 기기는 소정의 불법 복제 방지 프로토콜(예컨대, 5C DTCP)이 정하는 과정에 따라서 상호인증과정을 거친다. 상호인증과정이 성공하면 소오스 기기와 싱크 기기 사이에 안전한 디지털 암호채널을 형성하기 위한 암호/해독키를 서로 교환하고(단계③), 반대로 상호인증과정이 실패하면 소오스 기기는 싱크 기기가 신뢰할 수 없는 기기로 판단하고 콘텐츠 스트림의 전송을 중단한다. 위에서 암호채널이 형성된 경우, 이 암호채널을 통해서 소오스 기기와 싱크 기기는 콘텐츠 스트림을 주고받는다.

이와 같은, 종래의 기술에 의한 불법 복제 방지 프로토콜에서는 싱크 기기가 수신되는 콘텐츠 스트림의 저작권 정보를 분석하여 이 정보가 "copy-free"가 아닌 경우에는 이 콘텐츠 스트림이 암호화되어 있는 것으로서 현재로는 무용한 것으로 판단하고 소오스 기기로 상호인증을 요구하게 되어 있다. 이에 따라서, 불법 복제 기기는 수신되는 콘텐츠 스트림의 저작권 정보가 "copy-free"가 아닌 경우에 상호인증과정을 거치지 않고 암호화된 콘텐츠 스트림을 해독하려고 시도하는 경우에는 불법 복제 기기에게 취약하게 된다. 예컨대, 싱크 기기(불법 복제 기기)가 수신되는 콘텐츠 스트림을 가만히 관찰하기만 할 뿐 소오스 기기로 어떠한 신호도 보내지 않게 되면, 소오스 기기는 콘텐츠 스트림을 싱크 기기로 계속하여 전송하게 된다. 그러면, 싱크 기기(불법 복제 기기)에서는 암호화된 사이퍼텍스트(ciphertext)를 처음부터 끝까지 복사해 두었다가 나중에 시간을 가지고 반복해서 어택(attack)을 시도해서 불법 복제될 수 있는 문제점이 있었다.

발명이 이루고자하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 상술한 문제점을 해결하기 위하여 불법 복제로부터 보호의 필요성이 있는 콘텐츠가 디지털 인터페이스를 통하여 소오스 기기와 싱크 기기 사이에서 전달됨에 있어서 소정의 불법 복제 방지 프로토콜을 따르지 않는 싱크 기기의 불법 복제 시도를 무력화시킬 수 있는 불법 복제 방지를 위한 디지털 인터페이스 방법을 제공하는데 있다.

발명의 구성 및 작용

상기 기술적 과제를 달성하기 위하여 본 발명의 제1실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법은 콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인터페이스 방법에 있어서, (a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계, (b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 암호화하는 단계, (c) 상기 단계(b)의 암호화된 콘텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계 및 (d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상호인증요구가 수신되지 않는 경우에 상기 소오스에서 상기 콘텐츠의 전송을 중단하는 단계를 포함하는 것을 특징으로 한다.

상기 기술적 과제를 달성하기 위하여 본 발명의 제2실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법은 콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인터페이스 방법에 있어서, (a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계, (b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 암호화하는 단계, (c) 상기 단계(b)의 암호화된 콘

텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계, (d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상호인증요구가 수신되지 않는 경우에 상기 소오스에서 상기 싱크 기기로 상호인증요구를 전송하는 단계 및 (e) 상기 단계(c)의 상호인증요구 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상기 상호인증요구에 상응하는 정보가 수신되지 않는 경우에 상기 소오스에서 상기 콘텐츠의 전송을 중단하는 단계를 포함하는 것을 특징으로 한다.

상기 기술적 과제를 달성하기 위하여 본 발명의 제3실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법은 콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인터페이스 방법에 있어서, (a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계, (b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 소정의 키(key)로 암호화하는 단계, (c) 상기 단계(b)의 암호화된 콘텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계 및 (d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과할 때마다 상기 소정의 키(key)를 변경시키는 단계를 포함하는 것을 특징으로 한다.

이하 첨부된 도면을 참조하여 본 발명의 바람직한 실시 예에 대하여 상세히 설명하고자 한다.

도 3은 본 발명이 적용되는 IEEE 1394 네트웍 구성도의 일 실시 예로서, 디지털 TV(300), 셋톱박스(310), 디지털 TV(300) 및 디지털 셋톱박스(310)에 포함된 암호화 모듈(320, 330)로 구성되며, 디지털 TV(300)와 디지털 셋톱박스(310)는 IEEE 1394 버스상에 연결되어 있으며, 디지털 TV(300)와 디지털 셋톱박스(310)는 상호 IEEE 1394 디지털 인터페이스에 의하여 콘텐츠의 송수신을 실행한다.

여기에서 디지털 셋톱박스(310)가 소오스 기기가 되며, 디지털 TV(300)가 싱크 기기가 된다.

그러면, 구체적으로 본 발명에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법을 도 4~도 6을 참조하여 설명하기로 한다.

도 4는 본 발명의 제1실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법의 프로토콜을 도시한 것이다. 이를 단계별로 나누어 설명하면 다음과 같다.

첫 번째 단계에서, 사용자가 싱크 기기인 디지털 TV(300)의 리모콘 키를 입력하여 소오스 기기인 디지털 셋톱박스(310)에 콘텐츠 전송 요구를 전송한다.

두 번째 단계에서, 디지털 셋톱박스(310)는 전송 요구를 받은 콘텐츠의 저작권 정보를 조사하여 이 정보가 "copy-free"가 아닌 경우 소정의 암호 키값으로 암호화 모듈(320)에 의하여 콘텐츠 스트림을 암호화하여 디지털 인터페이스를 거친 후에 IEEE 1394 버스로 이용하여 싱크 기기인 디지털 TV(300)로 전송한다. 이 소정의 암호 키에 대해서는 종래의 불법 복제 방지 프로토콜에도 구체적으로 언급이 없으나, 임의의 랜덤 번호(random number)를 발생시켜 사용할 수 있다.

세 번째 단계에서, 소오스 기기인 디지털 셋톱박스(310)는 콘텐츠 스트림을 전송하기 시작한 이후부터 카운팅 또는 시간을 체크하여 소정의 시간이 경과하도록 싱크 기기인 디지털 TV(300)로부터 적법한 상호인증요구가 수신되지 않는 경우에는 싱크 기기가 불법 복제를 시도하는 것으로 판단하여 콘텐츠 스트림 전송을 중단한다. 여기에서 소정의 시간은 싱크 기기인 디지털 TV(300)에서 수신되는 콘텐츠 스트림을 분석하여 "copy-free" 여부를 판단하고 상호인증을 요구하기 위한 시간에 일정한 마진을 부가한 시간으로 결정한다.

위에서 설명한 제1실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법은 소오스 기기가 콘텐츠 스트림을 전송한 후 소정의 시간이 경과하도록 싱크 기기로부터 상호인증요구가 수신되지 않는 경우에 소오스 기기가 콘텐츠 스트림의 전송을 중단하는 방법을 사용하였다. 이 방법은 간단하기는 하지만 싱크 기기가 어떤 특별한 이유로 인하여 이 소정의 시간동안에 응답할 수 없었던 경우에는 불법 복제를 위한 목적이 아니었음에도 콘텐츠의 전송을 받을 수 없는 단점이 있다.

이러한 단점을 보완한 방법이 본 발명의 제2실시 예에 의한 불법 복제 방지를 위한 디지털 인터페이스 방법이며, 도5에 이에 대한 프로토콜을 도시하였다. 이를 단계별로 나누어 설명하면 다음과 같다.

첫 번째 단계에서, 사용자가 싱크 기기인 디지털 TV(300)의 리모콘 키를 입력하여 소오스 기기인 디지털 셋톱박스(310)에 콘텐츠 전송 요구를 전송한다.

두 번째 단계에서, 디지털 셋톱박스(310)는 전송 요구를 받은 콘텐츠의 저작권 정보를 조사하여 이 정보가 "copy-free"가 아닌 경우 소정의 암호 키값으로 암호화 모듈(320)에 의하여 콘텐츠 스트림을 암호화하여 디지털 인터페이스를 거친 후에 IEEE 1394 버스로 이용하여 싱크 기기인 디지털 TV(300)로 전송한다.

세 번째 단계에서, 소오스 기기인 디지털 셋톱박스(310)는 콘텐츠 스트림을 전송하기 시작한 이후부터 카운팅 또는 시간을 체크하여 소정의 시간이 경과하도록 싱크 기기인 디지털 TV(300)로부터 적법한 상호인증요구가 수신되지 않는 경우에는 제1실시 예에서와 같이 콘텐츠의 전송을 중단시키지 않고, 디지털 셋톱박스(310)에서 싱크 기기인 디지털 TV(300)로 상호인증요구를 전송한다. 여기에서, 소오스 기기인 디지털 셋톱박스(310)는 암호화 키값을 변경하여 불법 복제에 효율적으로 대처할 수 있으며, 또한 디지털 셋톱박스(310)에 의한 상호인증요구를 보다 효율적으로 하기 위하여 인증요구를 담고있는 패킷에 긴급(urgent) 표식을 부가할 수 있다.

네 번째 단계에서, 소오스 기기인 디지털 셋톱박스(310)가 상호인증요구를 이후로 시간을 체크하여 싱크 기기가 정상적으로 응답할 수 있는 소정의 시간이 경과하도록 싱크 기기인 디지털 TV(300)로부터 적법한 응답이 들어오지 않는 경우에는 디지털 셋톱박스(310)는 콘텐츠 스트림 전송을 중단한다.

다음으로 위의 제1,2실시 예에 비하여 간단한 방법인 제3실시 예를 도 6을 참조하여 설명하기로 한다. 이를 단계별로 나누어 설명하면 다음과 같다.

첫 번째 단계에서, 사용자가 싱크 기기인 디지털 TV(300)의 리모콘 키를 입력하여 소오스 기기인 디지털 셋톱박스(310)에 콘텐츠 전송 요구를 전송한다.

두 번째 단계에서, 디지털 셋톱박스(310)는 전송 요구를 받은 콘텐츠의 저작권 정보를 조사하여 이 정보가 "copy-free"가 아닌 경우 소정의 암호 키값으로 암호화 모듈(320)에 의하여 콘텐츠 스트림을 암호화하여 디지털 인터페이스를 거친 후에 IEEE 1394 버스로 이용하여 싱크 기기인 디지털 TV(300)로 전송한다.

세 번째 단계에서, 소오스 기기인 디지털 셋톱박스(310)는 콘텐츠 스트림을 전송하기 시작하고 나서, 싱크 기기인 디지털 TV(300)로부터 상호인증요구가 수신될 때까지 소정의 시간이 경과할 때마다 암호화 모듈의 암호 키를 변경한다. 이 암호 키 변경 주기는 일정할 수도 있고, 변경될 수도 있다.

발명의 효과

상술한 바와 같이, 본 발명에 의하면 불법 복제로부터 보호할 필요성이 있는 콘텐츠가 디지털 인터페이스를 통해 소오스 기기와 싱크 기기 사이에서 전송되는 경우에 싱크 기기가 불법 복제 방지 프로토콜에 따라 일정 시간이내에 상호인증요구를 송신하지 않으면 콘텐츠의 전송 중단, 소오스 기기에서 싱크 기기로의 상호인증요구, 또는 암호 변경 등을 실행함으로써, 불법 복제 시도를 무력화시킬 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1

콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인터페이스 방법에 있어서,

(a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계;

(b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 암호화하는 단계;

(c) 상기 단계(b)의 암호화된 콘텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계; 및

(d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상호인증요구가 수신되지 않는 경우에 상기 소오스에서 상기 콘텐츠의 전송을 중단하는 단계를 포함하는 것을 특징으로 하는 불법 복제 방지를 위한 디지털 인터페이스 방법.

청구항 2

콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인터페이스 방법에 있어서,

(a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계;

(b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 암호화하는 단계;

(c) 상기 단계(b)의 암호화된 콘텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계;

(d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상호인증요구가 수신되지 않는 경우에 상기 소오스에서 상기 싱크 기기로 상호인증요구를 전송하는 단계; 및

(e) 상기 단계(c)의 상호인증요구 전송 시점부터 소정의 시간이 경과하도록 상기 싱크 기기로부터 상기 소오스 기기로 상기 상호인증요구에 상응하는 정보가 수신되지 않는 경우에 상기 소오스에서 상기 콘텐츠의 전송을 중단하는 단계를 포함하는 것을 특징으로 하는 불법 복제 방지를 위한 디지털 인터페이스 방법.

청구항 3

제2항에 있어서, 상기 단계(d) 이후에 상기 소오스 기기에서 암호화 모듈의 암호 키를 변경시키는 단계를 더 포함함을 특징으로 불법 복제 방지를 위한 디지털 인터페이스 방법.

청구항 4

제2항에 있어서, 상기 단계(d)에서 상기 소오스 기기가 상호인증요구를 전송할 때 긴급 상황을 표시하는 식별표식을 부가해서 발송함을 특징으로 하는 불법 복제 방지를 위한 디지털 인터페이스 방법.

청구항 5

콘텐츠의 소오스 역할의 디지털 기기(소오스 기기)와 싱크 역할의 디지털 기기(싱크 기기)가 디지털 인터페이스로 연결되어 있고, 상기 소오스 기기로 상기 콘텐츠의 전송 요구가 수신되는 경우의 디지털 인

터페이스 방법에 있어서,

(a) 상기 소오스 기기가 전송 요구를 받은 상기 콘텐츠의 저작권 정보를 조사하는 단계;

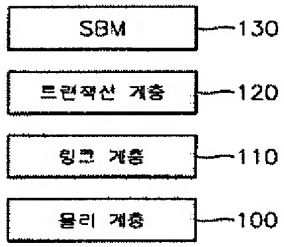
(b) 상기 단계(a)의 조사 결과 상기 저작권 정보가 자유로이 복제가 가능하다는 내용이 아닌 경우에, 상기 콘텐츠의 스트림을 소정의 키(key)로 암호화하는 단계;

(c) 상기 단계(b)의 암호화된 콘텐츠 스트림에 상기 저작권 정보를 부가하여 전송하는 단계; 및

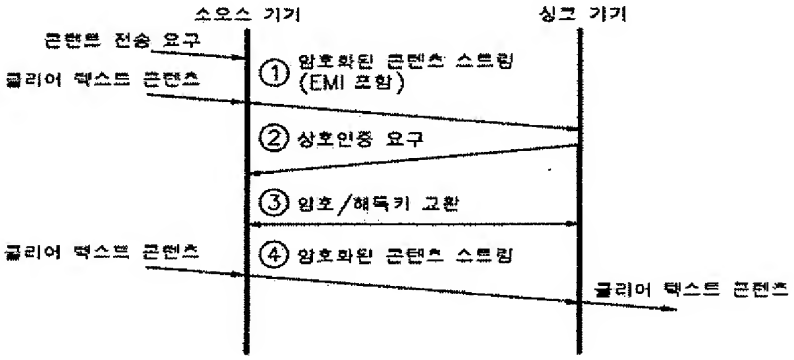
(d) 상기 단계(c)의 콘텐츠 스트림 전송 시점부터 소정의 시간이 경과할 때마다 상기 소정의 키(key)를 변경시키는 단계를 포함하는 것을 특징으로 하는 불법 복제 방지를 위한 디지털 인터페이스 방법.

도면

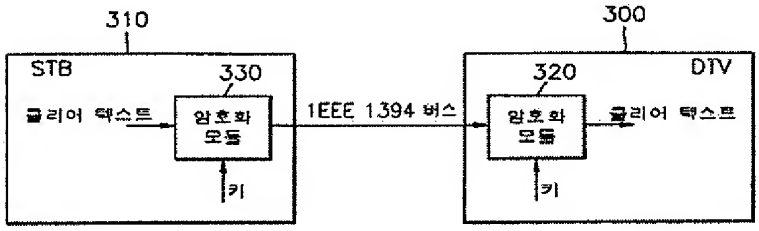
도면1



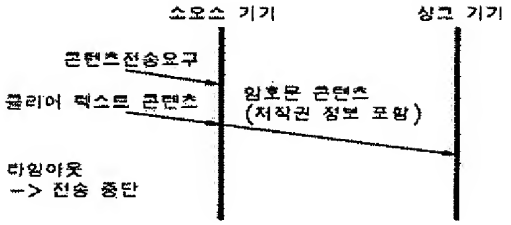
도면2



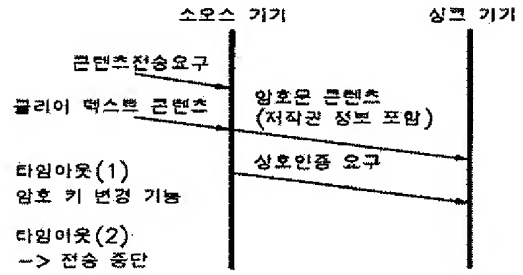
도면3



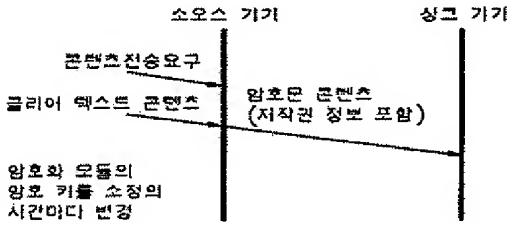
도면4


소오스 기기
싱크 기기
콘텐츠전송요구
클리어 텍스트 콘텐츠
암호문 콘텐츠
(저작권 정보 포함)
타임아웃
-> 전송 종단

도면5


소오스 기기
싱크 기기
콘텐츠전송요구
클리어 텍스트 콘텐츠
암호문 콘텐츠
(저작권 정보 포함)
상호인증 요구
타임아웃(1)
암호 키 변경 기능
타임아웃(2)
-> 전송 종단

도면6


소오스 기기
싱크 기기
콘텐츠전송요구
클리어 텍스트 콘텐츠
암호문 콘텐츠
(저작권 정보 포함)
암호화 모듈의
암호 키를 소정의
시간마다 변경

(19) Korean Intellectual Property Office (KR)
(12) Patent Laid-Open Publication (A)

(51) Int. Cl.[6]
H04L 9/00

(11) Laid-Open Publication No.: 10-2001-0004137
(43) Laid-Open Publication Date: January 15, 2001

(21) Application No.: 10-1999-0024751
(22) Filing Date: June 28, 1999

(71) Applicant: Samsung Electronics Co., Ltd. Yoon, Jong Yong
Gyeonggido Suwan Paldal-gu Maetan 3dong 416
(72) Inventors: Kim, Do Hyeong
Gyeonggido Hwasung-gun Bongdam myeon Sugiri 1-93
(74) Attorney(s): Lee, Young Phil
Gyon, Seock Heum
Lee, Sang Yong

Request for examination: *Not filed*

(54) Digital Interface Method for Preventing Illegal Copy

[Abstract]

The present invention relates to a digital interface method, more specifically to a digital interface method for preventing illegal copy when an illegal copy attempt is made without following the valid protocol process for copyright protection, with the provision that a source apparatus and a sink apparatus are connected through a digital interface.

According to the present invention, when a content to be protected from illegal copy is being transmitted between the source and sink devices through the digital interface, unless the sink device transmits a mutual authentication request within a predetermined period of time under illegal copy prevention protocol, the content transmission is discontinued, or the mutual authentication request is made from the source device to the sink device, or the password is changed, thereby baffling any illegal copy attempt.

Representative Figure: Fig. 4

Specification

Brief Description of Drawings

Fig. 1 shows an IEEE 1394 protocol stack.
Fig. 2 shows a basic structure of a digital transmission content protection protocol to prevent illegal copy according to related art.
Fig. 3 is a configuration diagram of an IEEE 1394 network according to one embodiment for implementing the present invention.
Fig. 4 shows a protocol structure to explain a digital interface method for preventing illegal copy according to a first embodiment of the present invention.
Fig. 5 shows a protocol structure to explain a digital interface method for preventing illegal copy according to a second embodiment of the present invention.
Fig. 6 shows a protocol structure to explain a digital interface method for preventing illegal copy according to a third embodiment of the present invention.

Detailed Description of the Invention

Objective(s) of the Invention

Technical Field of the Invention and Related art

The present invention relates to a digital interface method, more specifically to a digital interface method for preventing illegal copy when an illegal copy attempt is made without following the valid protocol process for copyright protection, with the provision that a source apparatus and a sink apparatus are connected through a digital interface.

Recently, there have come forth a variety of digital devices such as digital TVs, digital VCRs, digital setup boxes, etc., and an IEEE 1394 network is now drawing a lot of attention as it enables interface communications between these digital devices.
Fig. 1 shows an IEEE 1394 protocol stack, and a general protocol stack adopted to all devices that use a 1394 communication function includes a physical layer (100) as a lowermost layer, a link layer (110), a transaction layer (120) and a serial bus management (130) as an uppermost layer. The physical layer (100) receives a bit stream from the link layer (110) at the time of transmission, encodes and converts it into an electric signal after acquiring an access of the serial bus, and transmits data over an external bus. The opposite procedure takes place at the time of receiving. The link layer (110) handles data in packet unit and has functions of packet composition and decomposition, error detection and bus cycle management. In general, the physical layer (100) and the link layer (110) consist of chipsets. The transaction layer (120) provides transactions such as data read/write/lock and perform asynchronous communications with other devices (or nodes) that are placed on the 1394 bus using the service provided by a lower layer. The serial bus management (130) has several of built-in data structures such as configuration ROM, CSR (Control and Status Register), etc., and is in charge of power management and management of the uppermost layer such as connection structure/speed map, etc., of the entire system connected on the bus. The transaction layer (120) and the serial bus management layer (130) are written by software and are implemented by being built in a microprocessor of each device.

When a source device and a sink device are connected through such an IEEE 1394 digital interface and if a content being delivered between them requires copyright protection, the source and sink devices undergo a mutual authentication procedure between each other to form a safe pass-through channel and deliver the content through the pass-through channel.

Fig. 2 is a related art basic structure of a digital transmission contents protection protocol that is being discussed worldwide to prevent illegal copy.

That is, when a content transmission request is delivered from the sink device to the source device at early phase, the source device looks at encryption mode indicator (EMI) to be transmitted and if the indicator is not "copy-free" but requires copyright protection, it encrypts the stream of the content with an encryption module and attaches thereto the EMI and transmits it to the sink device through a digital interface such as IEEE 1394 (step ①). Then, the sink device looks at the EMI of the received content stream and if the EMI is not "copy-free", meaning that the content stream is encrypted and useless at the moment, the sink device requires the source device of mutual authentication (step ②). If the mutual authentication request is sent from the sink device to the source device, the sink and source devices undergo a mutual authentication procedure following the procedure given by a predetermined illegal copy prevention protocol (e.g., 5C DTCP). When the mutual authentication procedure succeeds, the source and sink devices exchange an encryption/decoding key for forming a safe digital pass-through channel (step ③). On the contrary, if the mutual authentication procedure fails, the source device decides that the sink device is not a reliable device and stops transmission of the content stream. If the pass-through channel is formed, the source device and the sink device exchange the content stream through this pass-through channel.

Therefore, in the illegal copy prevention protocol according to related art, the sink device analyzes EMI of a received content stream and if the EMI is not "copy-free", it regards that the content stream is encrypted and useless at the moment, so it requires the source device of mutual authentication. Accordingly, particularly when an illegal copy device attempts to decode an encrypted content stream without undergoing the mutual authentication procedure although EMI of a received content stream is not "copy-free", the related art protocol becomes vulnerable to that illegal copy device. For example, if the sink device (the illegal copy device) simply watches a content stream being received and does not send any signal to the source device, the source device continues transmission of the content stream. Then, the sink device (the illegal copy device) copies the ciphertext to the end from the beginning and repeatedly attacks it later, even if it takes some time, and succeeds in the illegal copy after all.

Technical Task to be Achieved by the Invention

To solve the above described problems, an object of the present invention is to provide a digital interface method for preventing illegal copy to baffle any attempt of illegal copy of a sink device that does not follow a predetermined illegal copy prevention protocol, when a content to be protected from the illegal copy is delivered between a source device and the sink device through a digital interface.

Construction and Operation of the Invention

To achieve the above described objects, according to a digital interface method for preventing illegal copy according to a first embodiment of the present invention, in a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device includes the steps of: (a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit; (b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content; (c) adding the EMI to the encrypted content stream in the step (b) and transmitting;

and (d) if a mutual authentication request is not received from the sink device to the source device until a predetermined amount of time from the start point of the content stream transmission in the step (c) has lapsed, the source device stopping transmission of the content.

To achieve the above described objects, according to a digital interface method for preventing illegal copy according to a second embodiment of the present invention, in a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device includes the steps of: (a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit; (b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content; (c) adding the EMI to the encrypted content stream in the step (b) and transmitting; (d) if a mutual authentication request is not received from the sink device to the source device until a predetermined amount of time from the start point of the content stream transmission in the step (c) has lapsed, the source device transmitting a mutual authentication request to the sink device; and (e) if information that corresponds to the mutual authentication request from the sink device to the source device is not received until a predetermined amount of time from the start point of the mutual authentication request transmission in the step (c) has lapsed, the source device stopping transmission of the content.

To achieve the above described objects, according to a digital interface method for preventing illegal copy according to a third embodiment of the present invention, in a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device includes the steps of: (a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit; (b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content with a predetermined key; (c) adding the EMI to the encrypted content stream in the step (b) and transmitting; and (d) changing the predetermined key whenever a predetermined amount of time elapses from the start point of the content stream transmission in the step (c).

Hereinafter, preferred embodiments of the present invention will be explained in detail with reference to accompanying drawings.

Fig. 3 shows one embodiment of the configuration of an IEEE 1394 network for implementing the present invention, which includes a digital TV (300), a set-top box (310), and encryption modules (320, 330) included in the digital TV (300) and the digital set-top box (310). The digital TV (300) and the digital set-top box (310) are connected over the IEEE 1394 bus, and the digital TV (300) and the digital set-top box (310) execute transmission and receiving contents through a mutual IEEE 1394 digital interface.

Here, the digital set-top box (310) becomes a source device, and the digital TV (300) becomes a sink device.

Next, a digital interface method for preventing illegal copy according to the present invention is explained in more details with reference to Fig. 4 through Fig. 6.

Fig. 4 shows a protocol based on a digital interface method for preventing illegal copy according to a first embodiment of the present invention. It will now be explained stepwisely as follows.

In the first step, a user inputs a remote control key of the digital TV (300), the sink device, to

transmit a content transmission request to the digital set-top box (310), the source device.

In the second step, the digital set-top box (310) exams EMI of a requested content and if the EMI is not "copy-free", it encrypts a content stream by the encryption module (320) with a predetermined password key value and lets it go through a digital interface, to transmit to the digital TV (300) via the IEEE 1394 bus. Although this predetermined password key has not been mentioned in the related art illegal copy prevention protocol, an arbitrary random number may be generated for use.

In the third step, the digital set-top box (310), the source device, counts or checks time from the start of transmission of the content stream and if no legal mutual authentication request is received from the digital TV (300), the sink device, until a predetermined amount of time has lapsed, it decides that the sink device is attempting the illegal copy so it stops the transmission of the content stream. Here, the predetermined amount of time corresponds to time required for requesting mutual authentication after the source device analyzes the received content stream from the digital TV (300), the sink device, and decides whether it is "copy-free", plus a certain margin.

The digital interface method for preventing illegal copy according to the first embodiment of the present invention allows the source device to stop the transmission of a content stream in case that no mutual authentication request is received from the sink device after a lapse of a predetermined amount of time from the start of transmission of the content stream from the source device. Although this method is simple, it has a shortcoming in that a sink device may not be able to receive a desired content when the sink device failed to respond within the predetermined amount of time for a certain reason even if it has no intention of the illegal copy.

A digital interface method for preventing illegal copy according to a second embodiment of the present invention is a method for completing such a shortcoming, and its protocol is shown in Fig. 5. It will now be explained stepwisely as follows.

In the first step, a user inputs a remote control key of the digital TV (300), the sink device, to transmit a content transmission request to the digital set-top box (310), the source device.

In the second step, the digital set-top box (310) exams EMI of a requested content and if the EMI is not "copy-free", it encrypts a content stream by the encryption module (320) with a predetermined password key value and lets it go through a digital interface, to transmit to the digital TV (300) via the IEEE 1394 bus.

In the third step, the digital set-top box (310), the source device, counts or checks time from the start of transmission of the content stream and if no legal mutual authentication request is received from the digital TV (300) until a predetermined amount of time has lapsed, instead of stopping transmission of a content as in the first embodiment, the digital set-top box (310) transmits a mutual authentication request to the digital TV (300), the sink device. Here, the digital set-top box (310), the source device, may change an encryption key value to efficiently handle the illegal copy, or may add an urgent mark to a packet conveying the authentication request to more efficiently make the mutual authentication request.

In the fourth step, the digital set-top box (310), the source device, checks time elapsed from its making the mutual authentication request, and if no legal response is received from the digital TV (300), the sink device, until a predetermined amount of time given to the sink device to be able to respond normally has lapsed, it stops transmission of the content stream.

Next, a third embodiment which is a relatively simple method, compared to the above first and

second embodiments, will now be explained with reference to Fig. 6. It will now be explained stepwisely as follows.

In the first step, a user inputs a remote control key of the digital TV (300), the sink device, to transmit a content transmission request to the digital set-top box (310), the source device.

In the second step, the digital set-top box (310) exams EMI of a requested content and if the EMI is not "copy-free", it encrypts a content stream by the encryption module (320) with a predetermined password key value and lets it go through a digital interface, to transmit to the digital TV (300) via the IEEE 1394 bus.

In the third step, the digital set-top box (310), the source device, starts transmitting the content stream and then changes a password key of the encryption module whenever a predetermined amount of time elapses until a mutual authentication request is received from the digital TV (300), the sink device. This password key change cycle may be fixed or variable.

Effects of the Invention

As has been described above, according to the present invention, when a content to be protected from illegal copy is being transmitted between the source and sink devices through the digital interface, unless the sink device transmits a mutual authentication request within a predetermined period of time under illegal copy prevention protocol, the content transmission is discontinued, or the mutual authentication request is made from the source device to the sink device, or the password is changed, thereby baffling any illegal copy attempt.

(57) What is claimed is:

1. In a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device comprising the steps of:
(a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit;
(b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content;
(c) adding the EMI to the encrypted content stream in the step (b) and transmitting; and
(d) if a mutual authentication request is not received from the sink device to the source device until a predetermined amount of time from the start point of the content stream transmission in the step (c) has lapsed, the source device stopping transmission of the content.

2. In a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device comprising the steps of:
(a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit;
(b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content;
(c) adding the EMI to the encrypted content stream in the step (b) and transmitting;
(d) if a mutual authentication request is not received from the sink device to the source device until

a predetermined amount of time from the start point of the content stream transmission in the step (c) has lapsed, the source device transmitting a mutual authentication request to the sink device; and

(e) if information that corresponds to the mutual authentication request from the sink device to the source device is not received until a predetermined amount of time from the start point of the mutual authentication request transmission in the step (c) has lapsed, the source device stopping transmission of the content.

3. The method of claim 2, further comprising, after the step of (d), the step of:
the source device changing a password key of an encryption module.

4. The method of claim 2, wherein when the source device transmits the mutual authentication request, it adds an identification mark for displaying an urgent situation to the request to be sent.

5. In a digital device (source device) functioning as a source of a content and in a digital device (sink device) functioning as a sink being connected to each other with a digital interface, a digital interface method in case a transmission request of the content is sent to the source device comprising the steps of:

(a) the source device examining Encryption Mode Indicator (EMI) of the content being requested to transmit;

(b) if the EMI is not copy-free according to the examination result in the step (a), encrypting a stream of the content with a predetermined key;

(c) adding the EMI to the encrypted content stream in the step (b) and transmitting; and

(d) changing the predetermined key whenever a predetermined amount of time elapses from the start point of the content stream transmission in the step (c).

Description of Drawings

Fig. 1

트랜잭션 계층 120: Transaction layer 120
링크 계층 110: Link layer 110
물리 계층 100: Physical layer 100

Fig. 2

소오스 기기: Source device
싱크 기기: Sink device
콘텐트 전송 요구: Content transmission request
클리어 텍스트 콘텐츠: Clear text content
① 암호화된 콘텐츠 스트림 (EMI 포함): Encrypted content stream (including EMI)
② 상호인증 요구: Mutual authentication request
③ 암호/해독키 교환: Exchange password/decoding key
④ 암호화된 콘텐츠 스트림: Encrypted content stream

Fig. 3

클리어 텍스트: Clear text
암호화 모듈 330: Encryption module
IEEE 1394 버스: IEEE 1394 bus
암호화 모듈 320: Encryption module
키: Key

Fig. 4

소오스 기기: Source device
싱크 기기: Sink device
콘텐트 전송 요구: Content transmission request
클리어 텍스트 콘텐츠: Clear text content
암호문 콘텐츠 (저작권 정보 포함): Encryption content (including EMI)
타임 아웃 -> 전송 중단: Time-out -> Stop transmission

Fig. 5

소오스 기기: Source device
싱크 기기: Sink device
콘텐트 전송 요구: Content transmission request
클리어 텍스트 콘텐츠: Clear text content
암호문 콘텐츠 (저작권 정보 포함): Encryption content (including EMI)
타임 아웃 (1) -> 암호 키 변경 기능: Time-out (1) -> Password key change function
타임 아웃 (2) -> 전송 중단: Time-out -> Stop transmission

Fig. 6

소오스 기기: Source device
싱크 기기: Sink device
콘텐트 전송 요구: Content transmission request
클리어 텍스트 콘텐츠: Clear text content
암호문 콘텐츠 (저작권 정보 포함): Encryption content (including EMI)
암호화 모듈의 암호 키를 소정의 시간마다 변경: Change password key of encryption module at every predetermined time

FIG. 1

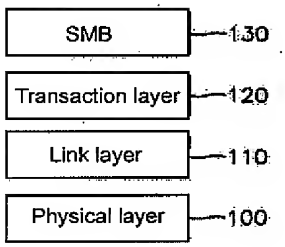


FIG. 2

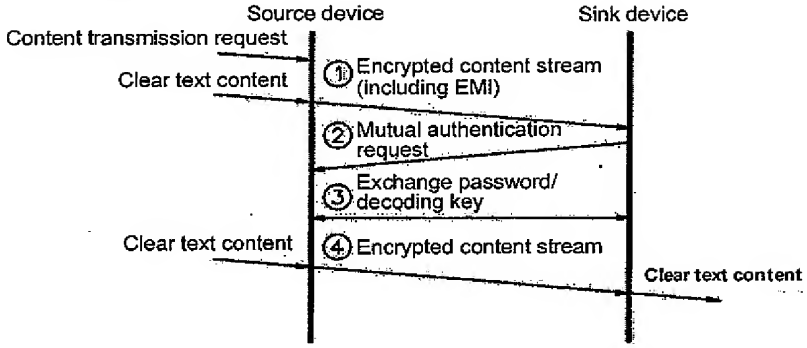


FIG. 3

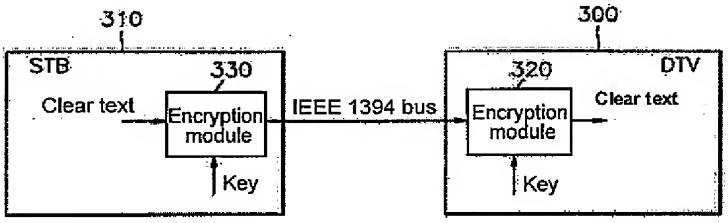


FIG. 4

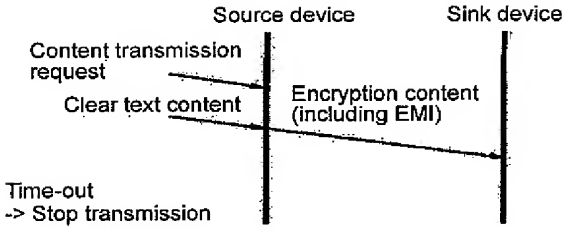


FIG. 5

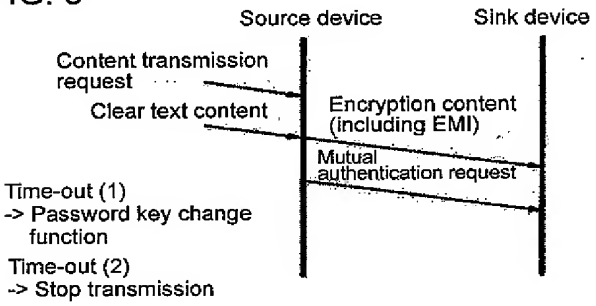


FIG. 6